

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/015209

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L12/28, G06F13/00, H04B7/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L12/28, G06F13/00, H04B7/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2003-152735 A (Seiko Epson Corp.), 23 May, 2003 (23.05.03), Par. Nos. [0032] to [0036], [0043]; Figs. 1 to 4 & US 2003/0092395 A1	1, 4-7 2, 3
Y	JP 2002-101459 A (NTT Comware Corp.), 05 April, 2002 (05.04.02), Par. Nos. [0032] to [0036]; Fig. 2 (Family: none)	2, 3
A	JP 2003-218875 A (Seiko Epson Corp.), 31 July, 2003 (31.07.03), Par. Nos. [0033] to [0036]; Figs. 1 to 3 (Family: none)	1-7

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
21 December, 2004 (21.12.04)

Date of mailing of the international search report
11 January, 2005 (11.01.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/015209

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-218730 A (Seiko Epson Corp.), 31 July, 2003 (31.07.03), Par. Nos. [0025] to [0026]; Figs. 1 to 4 (Family: none)	1-7

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/28, G06F13/00, H04B7/26

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/28, G06F13/00, H04B7/26

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2003-152735 A (セイコーエプソン株式会社) 2003.05.23, 【0032】-【0036】,	1,4-7
Y	【0043】, 図1-図4 & US 2003/0092395 A1	2,3
Y	JP 2002-101459 A (エヌ・ティ・ティ・コムウェア株式会社) 2002.04.05, 【0032】-【0036】, 図2 (ファミリーなし)	2,3

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

21.12.2004

国際調査報告の発送日

11.1.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中木 努

5X

9299

電話番号 03-3581-1101 内線 3596

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2003-218875 A (セイコーエプソン株式会社) 2003. 07. 31, 【0033】 - 【0036】, 図1-図3 (ファミリーなし)	1-7
A	J P 2003-218730 A (セイコーエプソン株式会社) 2003. 07. 31, 【0025】 - 【0026】, 図1-図4 (ファミリーなし)	1-7

明細書

無線通信端末および接続情報設定方法

技術分野

この発明は、無線通信端末および接続情報設定方法に関し、特にたとえば、メモリに保存された接続情報を用いてネットワークのアクセスポイントに無線接続する無線通信端末に接続情報を設定する、無線通信端末および接続情報設定方法に関する。

従来技術

無線LAN(Local Area Network)のアクセスポイントに無線接続するために必要な接続情報をキーボードやマウスを用いてPC(Personal Computer)に設定する方法が、“「無線LANと高速インターネット」設定入門、村上俊一、株式会社メディア・テック出版、2003年5月”に詳細に開示されている。

しかし、この方法では、ポータブル音楽再生機やインターネットラジオ受信機のような、ディスプレイのサイズや操作キーの数が限られた機器に、接続情報を設定することは不可能である。

発明の概要

それゆえに、この発明の主たる目的は、新規な無線通信端末および接続情報設定方法を提供することである。

この発明の他の目的は、文字入力インタフェースを備えない無線通信端末に対して容易に接続情報の設定を行うことができる、無線通信端末および接続情報設定方法を提供することである。

クレーム1によれば、ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する無線通信端末は、次のものを備える：特定無線通信端末を識別する端末識別子を受け付ける受付手段；受付手段によって受け付けた端末識別子に基づいて特定無線通信端末と接続する接続手段；および接続手段による接続の後に接続情報を特定無線通信端末に転送する転送手段。

特定無線通信端末を識別する端末識別子が受付手段によって受け付けられると、接続手段は、この端末識別子に基づいて特定無線通信端末と接続する。転送手段は、接続手段による接続の後に、接続情報を特定無線通信端末に転送する。これによって、文字入力インタフェースを備えない特定無線通信端末に対して、ネットワークのアクセスポイントへの無線接続に必要な接続情報を容易に設定することができる。

クレーム 1 に従属するクレーム 2 によれば、特定無線通信端末はネットワークに接続された認証端末によって認証された電子証明書を有し、無線通信端末は、接続手段による接続の後に特定無線通信端末から電子証明書を取得する取得手段；および取得手段によって取得された電子証明書に基づいて特定無線通信端末が正規の端末であるか否かを判別する判別手段をさらに備え、転送手段は判別手段の判別結果が肯定的であるとき接続情報を転送する。

特定無線通信端末は、認証端末によって認証された電子証明書を有している。取得手段は、特定無線通信端末から電子証明書を取得し、判別手段は、取得手段によって取得された電子証明書に基づいて特定無線通信端末が正規の端末であるか否かを判断する。転送手段は判別手段の判別結果が肯定的であるとき、つまり、特定無線通信端末が正規の端末であるときに、接続情報を特定無線通信端末に転送する。したがって、不正な無線通信端末が接続情報を取得する事態を防止することができる。

クレーム 2 に従属するクレーム 3 によれば、電子証明書は認証端末のアドレスを含み、判別手段は、アドレスに従って認証端末にアクセスするアクセス手段、および特定無線通信端末の正当性の判別を認証端末に要求する要求手段を含む。この結果、無線通信端末は別途に認証端末のアドレスを取得する必要がある。

クレーム 1 に従属するクレーム 4 によれば、接続情報は、アクセスポイントを識別するアクセスポイント識別子を含む。これによって、文字入力インタフェースを有さない特定無線通信端末にアクセスポイントの識別情報を与えることができる。

クレーム 1 に従属するクレーム 5 によれば、接続情報は、アクセスポイントと暗号化通信を行うための暗号化鍵情報を含む。これによって、文字入力インタフ

エースを有さない特定無線通信端末に暗号化鍵を与えることができる。

クレーム 6 によれば、ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する接続情報設定方法は、次のステップを備える：(a)特定無線通信端末を識別する端末識別子を受け付け；(b)ステップ(a)で受け付けた端末識別子に基づいて特定無線通信端末と接続し；そして(c)接続情報を特定無線通信端末に転送する。

上述のクレーム 1 と同様、文字入力インタフェースを有さない特定無線通信端末に接続情報を容易に設定することができる。

クレーム 7 によれば、ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する無線通信端末のプロセッサによって実行される接続情報設定プログラムは、次のものを備える：特定無線通信端末を識別する端末識別子を受け付ける受付ステップ；受付ステップによって受け付けた端末識別子に基づいて特定無線通信端末を接続する接続ステップ；および接続ステップによる接続の後に接続情報を特定無線通信端末に転送する転送ステップ。

クレーム 1 と同様、文字入力インタフェースを有さない特定無線通信端末に対して接続情報を容易に設定することができる。

この発明の上述の目的、その他の目的、特徴および利点は、図面を参照して行う以下の実施例の詳細な説明から一層明らかとなろう。

図面の簡単な説明

図 1 はこの発明の一実施例の構成を示すブロック図であり；

図 2 は図 1 実施例に適用されるパーソナルコンピュータの構成の一例を示すブロック図であり；

図 3 は図 1 実施例に適用されるインターネットラジオ受信機の構成の一例を示すブロック図であり；

図 4 は図 2 実施例に適用される CPU および図 3 実施例に適用される MCU の動作の一部を示すフロー図であり；そして

図 5 は図 2 実施例に適用される CPU および図 3 実施例に適用される MCU の動作の他の一部を示すフロー図である。

発明を実施するための最良の形態

図1を参照して、この実施例のPC10は、無線通信によって無線LANアクセスポイントルータ30に接続可能である。インターネットラジオ受信機20と無線LANアクセスポイントルータ30との無線通信を可能にするための設定は、このPC10を利用して行われる。

無線LANアクセスポイントルータ30は、インターネット100に接続される。インターネット100上には、インターネットラジオ受信機20の認証を行うための認証サーバ40が存在する。なお、無線LANアクセスポイントルータ30は、ネットワークに接続された無線通信端末にIPアドレスなどのネットワーク情報を割り当てるDHCP(Dynamic Host Configuration Protocol)機能を有する。

インターネットラジオ受信機20の記憶装置には、認証サーバ40によって発行された電子証明書とこの電子証明書に含まれる公開鍵に対応する秘密鍵とが、製造の段階で書き込まれている。なお、電子証明書には、公開鍵の他に認証サーバ40のインターネット100上での場所を示すアドレス(URL: Uniform Resource Locator)が含まれている。

インターネットラジオ受信機20は、無線LANアクセスポイントルータ30を介してインターネット100に接続し、インターネット100上に存在するラジオ局(図示せず)から音楽などの音声コンテンツのストリーミング配信を受ける。

PC10は、具体的には、図2に示すように構成されている。図2によれば、PC10はCPU(Central Processing Unit)50を含む。CPU50は、バス64を介して、RAM(Random Access Memory)52, HDD(Hard Disc Drive)54, 無線LANカード56, ディスプレイ58, キーボード60およびマウス62と接続される。無線LANカード56は、EEPROM(Electronically Erasable PROM)56eを有する。CPU50は、HDD54に記録されたプログラムに従う処理を実行する。なお、HDD54は、インターネットラジオ受信機20を無線LANアクセスポイントルータ30に接続させるための設定を行う

アプリケーションプログラムAP 1を格納する。

また、インターネットラジオ受信機20は、具体的には、図3に示すように構成される。図3によれば、インターネットラジオ受信機20は、MCU(Micro Controller Unit)70を含む。MCU70は、ROM(Read Only Memory)72, RAM74, 無線LANカード76, キーパッド78およびDSP(Digital Signal Processor)80と接続される。ディスプレイ82は、DSP80と直接的に接続される。また、スピーカ88は、AMP(AMPlifier)86とDAC(Digital to Analog Converter)84とを介してDSP80と接続される。無線LANカード76には、EEPROM76eが設けられる。

キーパッド78は、電源キー78p, ラジオ局を選択するためのアップキー78uおよびダウンキー78d, 記憶している特定のラジオ局を選択するための複数のプリセットキー78sを備える。なお、キーボードのような文字を容易に入力できる入力インタフェースは、インターネットラジオ受信機20に用意されていない。MCU70は、ROM72に記録されたプログラムに従う処理を実行する。なお、ROM72は、インターネットラジオ受信機20を無線LANアクセスポイントルータ30に接続させるための設定を受け付けるアプリケーションプログラムAP2を格納する。また、ROM72には、上述の電子証明書および秘密鍵が記憶される。

SSID(Service Set Identifier)およびWEP(Wired Equivalent Privacy)鍵を接続情報として無線LANカード76に設定すれば、インターネットラジオ受信機20は、無線LANアクセスポイントルータ30との間で無線通信を行うことができる。

この実施例においては、このような無線通信を実現するために、IEEE802.11と呼ばれる仕様が採用される。この仕様は、無線LANシステム標準化に関するIEEE(Institute of Electrical and Electronics Engineers Inc.)の分科会によって規格化された仕様である。

IEEE802.11を用いた無線LAN通信では、SSIDというアクセスポイント識別子が、無線通信端末に割り当てられる。インフラストラクチャ(Infrastructure)モードに従う無線通信は、同じSSIDを有する無線通信端末間

においてのみ可能となる。したがって、P C 1 0、インターネットラジオ受信機 2 0 および無線アクセスポイントルータ 3 0 の間でインフラストラクチャモードでの無線通信を行うためには、P C 1 0、インターネットラジオ受信機 2 0 および無線アクセスポイントルータ 3 0 に同一の S S I D を設定する必要がある。

なお、インフラストラクチャモードは、無線アクセスポイントルータ 3 0 のようなアクセスポイントを介して無線通信端末どうしを接続するモードである。ちなみに、アクセスポイントを介さずに無線通信端末どうしを直接的に無線接続するモードは、アドホック(Ad-Hoc)モードと呼ばれる。アドホックモードの場合、所望の無線通信端末の間でのみ共通する S S I D の設定が必要となる。

また、I E E E 8 0 2 . 1 1 に準拠した無線LAN通信では、W E P と呼ばれるセキュリティアルゴリズムが用いられる。W E P アルゴリズムによれば、通信を行う各々の無線通信端末がW E P 鍵(暗号化鍵)を保持し、無線通信はW E P 鍵が互いに一致した場合にのみ可能となる。具体的には、無線通信端末から送信されるデータはこのW E P 鍵によって暗号化され、データを受信した無線通信端末では暗号化に用いられたW E P 鍵と同じW E P 鍵によって暗号化データが復号される。したがって、P C 1 0、インターネットラジオ受信機 2 0 および無線アクセスポイントルータ 3 0 の間での無線通信には、共通のW E P 鍵が使用される。

無線通信端末を購入して初めて利用する場合、あるいは今までと異なる無線LAN環境で無線通信端末を使用する場合、使用する無線LAN環境に固有の S S I D およびW E P 鍵を無線通信端末に設定する必要がある。無線LANに新たに接続する無線通信端末が図 1 に示すキーボード 6 0 のような優れた文字入力インタフェースを備えている場合、S S I D やW E P 鍵の設定は容易である。

しかし、無線LANに新たに接続する無線通信端末がインターネットラジオ受信機 2 0 のように文字入力インタフェースを備えていない場合、S S I D やW E P 鍵の設定は困難である。

そこで、この実施例では、P C 1 0 とインターネットラジオ受信機 2 0 とをアドホックモードで無線接続し、S S I D およびW E P 鍵をP C 1 0 によってインターネットラジオ受信機 2 0 の無線LANカード 7 6 に設定するようにしている。

具体的には、まず、インターネットラジオ受信機 2 0 にデフォルトとして設定

されているSSIDがPC10に設定される。PC10にはまた、インターネットラジオ受信機20にデフォルトとして設定されている固定IP(Internet Protocol)アドレスとネットワーク部のみが一致するIPアドレスが設定される。なお、デフォルトのSSIDおよび固定IPアドレスは、インターネットラジオ受信機20の取り扱い説明書から知得される。これによって、アドホックモードに従う無線接続が、PC10とインターネットラジオ受信機20との間で確立される。

無線接続が確立されると、PC10は、インターネットラジオ受信機20から電子証明書を取得し、取得した電子証明書に含まれている公開鍵が登録されているかどうかを認証サーバ40に問い合わせる。これによって、インターネットラジオ受信機20が正規の機器であることの確認や、WEP鍵などの不正取得の防止が可能となる。

インターネットラジオ受信機20の認証に成功すると、PC10は、自身が無線LANアクセスポイントルータ30との無線通信に使用しているSSIDおよびWEP鍵を、電子証明書から抽出した公開鍵を用いて暗号化する。暗号化されたSSIDおよびWEP鍵は、インターネットラジオ受信機20に送信される。送信処理が完了すると、PC10はインフラストラクチャモードに復帰する。

インターネットラジオ受信機20は、PC10から暗号化状態で送信されたSSIDおよびWEP鍵を、PC10に送信した公開鍵に対応する秘密鍵を用いて復号する。復号されたWEP鍵およびSSIDは、無線LANカード76に設定される。設定処理が完了すると、インターネットラジオ受信機20は、通信モードをインフラストラクチャモードに変更する。

こうしてインターネットラジオ受信機20の無線LANカード76に新たなSSIDおよびWEP鍵が設定されると、無線LANアクセスポイントルータ30との無線通信が可能となる。

インターネットラジオ受信機20にSSIDおよびWEP鍵を設定するとき、PC10のCPU50およびインターネットラジオ受信機20のMCU70は、図4および図5に示すフロー図に従う処理を実行する。

まず、ユーザは、インターネットラジオ受信機20に付属するCD-ROMを

用いて、SSIDおよびWEP鍵をインターネットラジオ受信機20に設定するためのアプリケーションプログラムAP1をPC10にインストールする。次に、ユーザは、マウス62を用いてディスプレイ58に表示されたアプリケーションプログラムAP1を起動するためのアイコンをダブルクリックする。

すると、PC10のCPU50は、ステップS1でアプリケーションプログラムAP1を起動する。ステップS3では、PC10の無線LANカード56に現時点で設定されているインフラストラクチャモード（ISモード）用のSSIDおよびIPアドレスをRAM52に退避する。

ユーザは、PC10のディスプレイ58に表示されるWebページのガイドに従って、アドホックモード（AHモード）用のSSIDおよび固定IPアドレスを入力する。入力されるSSIDおよび固定IPアドレスはそれぞれ、インターネットラジオ受信機20の無線LANカード76にデフォルトとして設定されているSSIDおよび固定IPアドレスであり、インターネットラジオ受信機20の取り扱い説明書から知得される。

入力されたSSIDおよび固定IPアドレスは、ステップS5およびS7でそれぞれ受け付けられる。SSIDは、そのまま無線LANカード56のEEPROM56eに書き込まれる。これに対して、固定IPアドレスはネットワーク部のみが一致するIPアドレスへの変換処理を施され、変換されたIPアドレスがEEPROM56eに書き込まれる。

AHモード用のSSIDおよびIPアドレスの設定が終了すると、PC10は、ステップS9でインフラストラクチャモードからアドホックモードに移行し、ステップS11でアドホックモードでの通信相手であるインターネットラジオ受信機20に対して認証要求を送信する。

インターネットラジオ受信機20のMCU70は、ステップS13で認証要求を受信し、セットアップのためのアプリケーションプログラムAP2をステップS15で起動する。ステップS17では、ROM72から電子証明書を読み出し、読み出された電子証明書をPC10に送信する。

PC10は、インターネットラジオ受信機20から送信された電子証明書をステップS19で受信する。ステップS21では、無線LANカード56に現時点

で設定されているAHモード用のSSIDおよびIPアドレスをRAM52に退避させ、先のステップS3でRAM52に退避されたISモード用のSSIDおよびIPアドレスを無線LANカード56に設定する。

ステップS25では通信モードをインフラストラクチャモードに変更し、ステップS27では無線LANアクセスポイントルータ30を介して認証サーバ40にアクセスする。なお、上述したように、認証サーバ40にアクセスするためのURLは、インターネットラジオ受信機20から受信した電子証明書に含まれている。

ステップS29では、電子証明書から抽出した公開鍵を認証サーバ40に送信し、公開鍵の有効性の判断を求める。図5のステップS31では、認証サーバ40から公開鍵の有効性の判断結果を受信する。受信処理が完了すると、認証サーバ40との接続をステップS33で切断する。

ステップS35では、公開鍵の有効性の判断結果が肯定的であるかどうか、つまり公開鍵が有効であるかどうかを判断する。ステップS35でNOであれば、ステップS53でエラー処理を行う。一方、ステップS35でYESであれば、ステップS37以降の処理に進む。公開鍵の有効性を確認することで、インターネットラジオ受信機20が正規の機器であることが認証される。

ステップS37では、無線LANカード56に設定されているISモード用のSSIDおよびIPアドレスをRAM52に退避する。ステップS39では、RAM52に退避されたAHモード用のSSIDおよびIPアドレスを無線LANカード56に設定する。ステップS41では、通信モードをアドホックモードに変更する。

ステップS43では、無線LANカード56のEEPROM56eに記録されているWEP鍵とRAM52に退避されているISモード用のSSIDとを、有効性が確認された公開鍵を用いて暗号化する。ステップS45では、暗号化されたWEP鍵およびISモード用のSSIDをインターネットラジオ受信機20に送信する。

暗号化されたWEP鍵およびISモード用のSSIDの送信が完了するとステップS47に進み、RAM52に退避されているISモード用のSSIDおよび

IPアドレスを無線LANカード56に設定する。ステップS49では通信モードをインフラストラクチャモードに変更し、ステップS51ではアプリケーションプログラムAP1を終了する。

一方、インターネットラジオ受信機20は、PC10から暗号化状態で送信されたWEP鍵およびISモード用のSSIDをステップS55で受信する。ステップS57では、ROM72から秘密鍵を読み出し、受信したWEP鍵およびISモード用のSSIDを読み出された秘密鍵を用いて復号する。復号されたWEP鍵およびISモード用のSSIDは、ステップS59で無線LANカード76のEEPROM76eに設定される。ステップS61では、通信モードをインフラストラクチャモードに変更する。

ステップS63では無線LANアクセスポイントルータ30にIPアドレスを要求し、ステップS65では無線LANアクセスポイントルータ30からIPアドレスを取得する。取得されたIPアドレスは無線LANカード76に設定される。設定が完了すると、ステップS67でアプリケーションプログラムAP2を終了する。

こうしてWEP鍵およびSSIDがインターネットラジオ受信機20に設定された結果、インターネットラジオ受信機20は、無線LANアクセスポイントルータ30を介してPC10やインターネット100に接続することができる。

以上の説明から分かるように、無線LANアクセスポイントルータ30との無線接続に必要な接続情報(SSID, WEP鍵など)は、キーボード60またはマウス62を用いてPC10に入力される。入力された接続情報は、PC10によってインターネットラジオ受信機20に設定される。したがって、無線接続に必要な接続情報を文字入力インタフェースを持たない無線通信端末に容易に設定することができる。

なお、この実施例では、無線通信接続の設定を行う機器としてインターネットラジオ受信機20を想定しているが、WEP鍵やSSIDのような接続情報を設定して無線通信を行う無線通信端末である限り、機器はインターネットラジオ受信機に限られない。また、図4および図5に示すPC10の処理動作を無線LANアクセスポイントルータ30に割り当てるようにしてもよい。

この発明が詳細に説明され図示されたが、それは単なる図解および一例として用いたものであり、限定であると解されるべきではないことは明らかであり、この発明の精神および範囲は添付されたクレームの文言によってのみ限定される。

;

請求の範囲

1. ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する無線通信端末であって、次のものを備える：

前記特定無線通信端末を識別する端末識別子を受け付ける受付手段；

前記受付手段によって受け付けた端末識別子に基づいて前記特定無線通信端末と接続する接続手段；および

前記接続手段による接続の後に前記接続情報を前記特定無線通信端末に転送する転送手段。

2. クレーム1に従属する無線通信端末であって、前記特定無線通信端末は前記ネットワークに接続された認証端末によって認証された電子証明書を有し、

前記無線通信端末は、前記接続手段による接続の後に前記特定無線通信端末から前記電子証明書を取得する取得手段；および前記取得手段によって取得された前記電子証明書に基づいて前記特定無線通信端末が正規の端末であるか否かを判別する判別手段をさらに備え、

前記転送手段は前記判別手段の判別結果が肯定的であるとき前記接続情報を転送する。

3. クレーム2に従属無線通信端末であって、前記電子証明書は前記認証端末のアドレスを含み、前記判別手段は、前記アドレスに従って前記認証端末にアクセスするアクセス手段、および前記特定無線通信端末の正当性の判別を前記認証端末に要求する要求手段を含む。

4. クレーム1に従属する無線通信端末であって、前記接続情報は、前記アクセスポイントを識別するアクセスポイント識別子を含む。

5. クレーム1に従属する無線通信端末であって、前記接続情報は、前記アクセスポイントと暗号化通信を行うための暗号化鍵情報を含む。

6. ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する接続情報設定方法であって、次のステップを備える：

(a) 前記特定無線通信端末を識別する端末識別子を受け付け、

(b) 前記ステップ(a)で受け付けた端末識別子に基づいて前記特定無線通信端末と接続し、そして

(c) 前記接続情報を前記特定無線通信端末に転送する。

7. ネットワークのアクセスポイントへの無線接続に必要な接続情報を特定無線通信端末に設定する無線通信端末のプロセサによって実行される接続情報設定プログラムであって、次のものを備える：

前記特定無線通信端末を識別する端末識別子を受け付ける受付ステップ；

前記受付ステップによって受け付けた端末識別子に基づいて前記特定無線通信端末を接続する接続ステップ；および

前記接続ステップによる接続の後に前記接続情報を前記特定無線通信端末に転送する転送ステップ。

図1

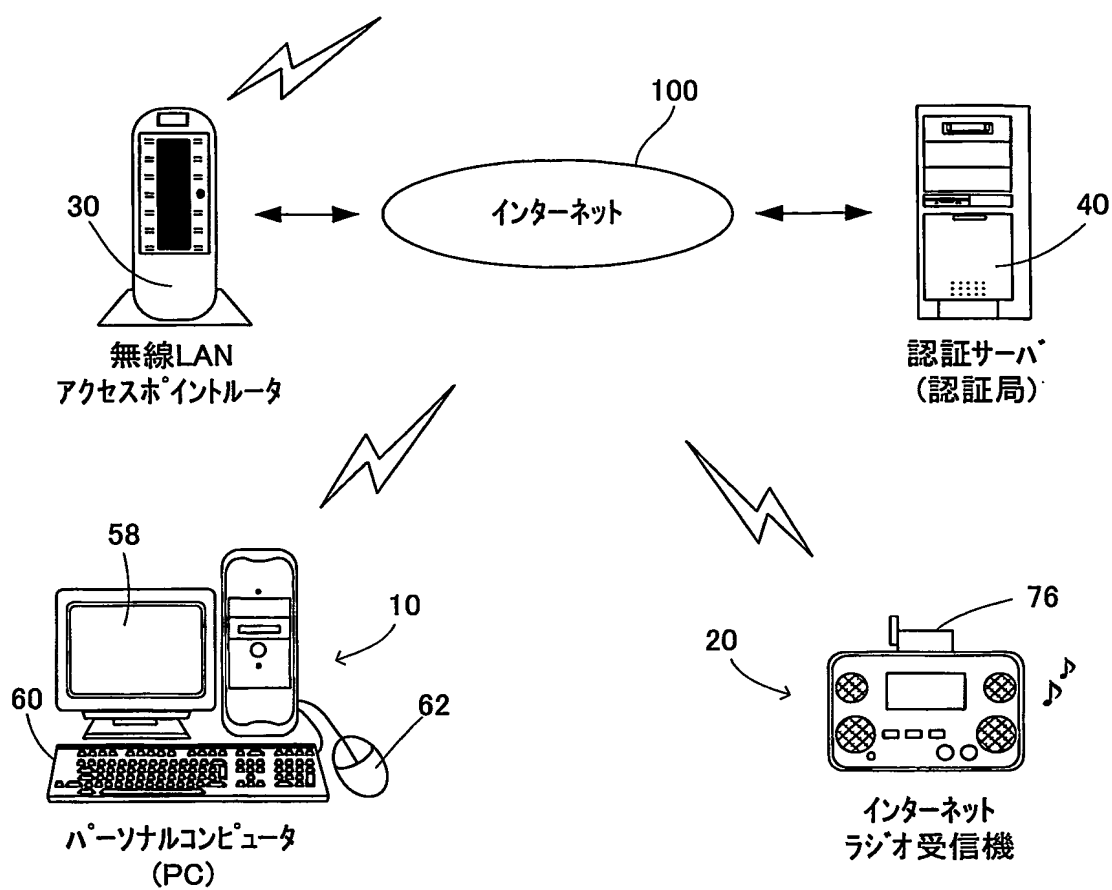


図2

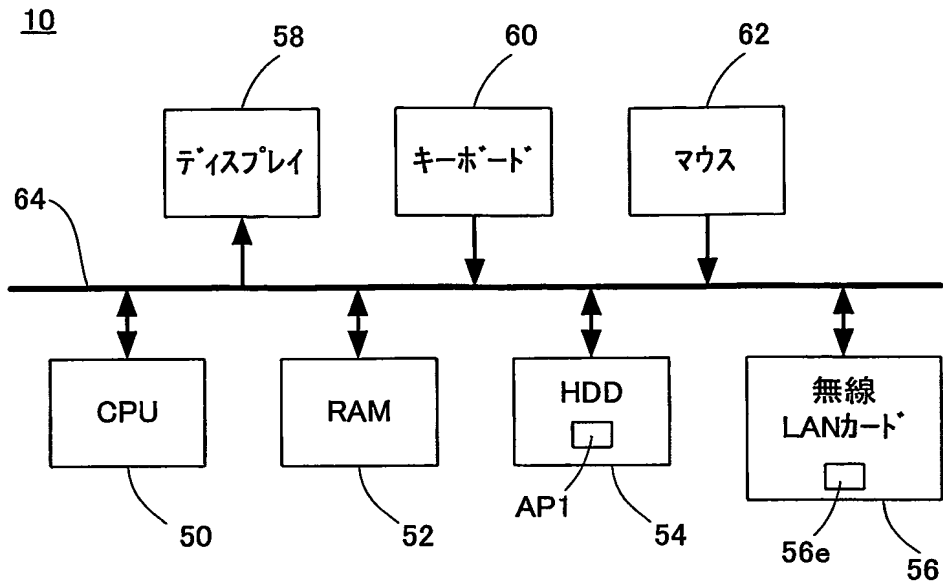


図3

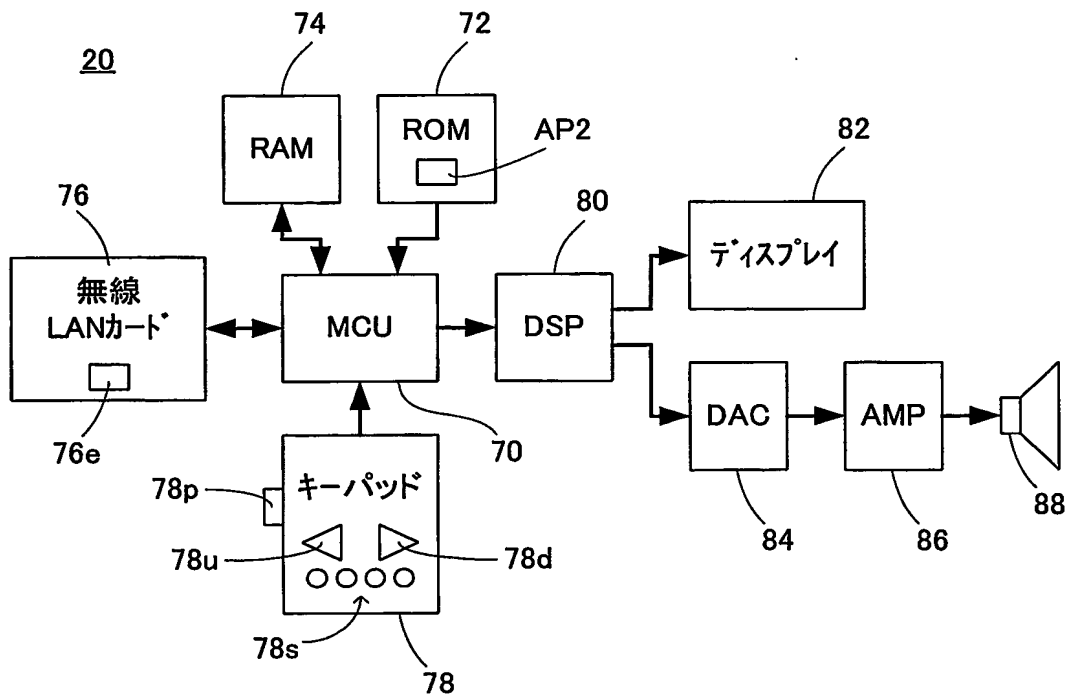


図4

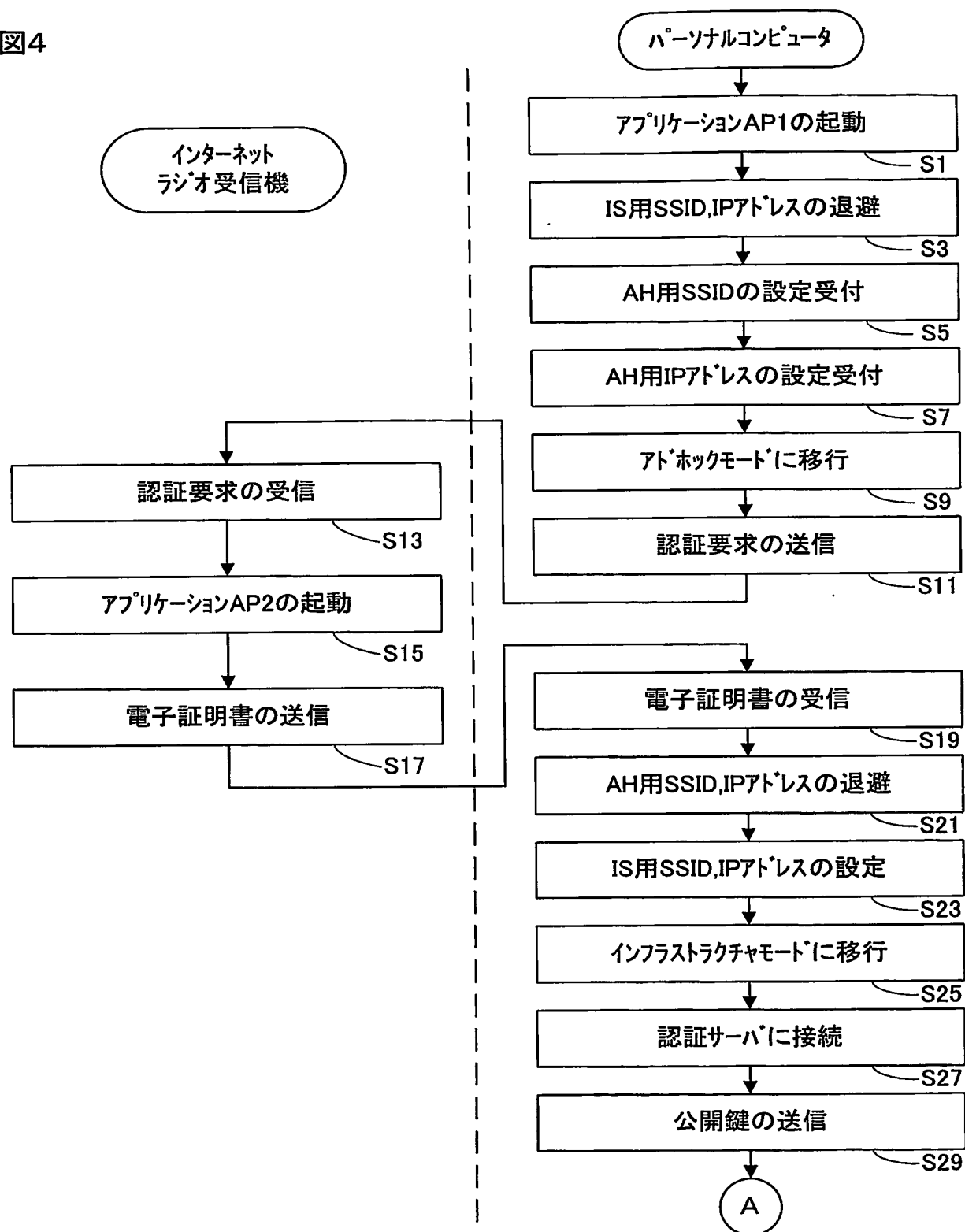


図5

